安全加社区

公益
译文
项目

2017

使用 STIX™ 规范
网络威胁情报信息

Sean Barnum

2014 年 2 月 20 日

MITRE

文档信息			
原文名称	Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression(STIX™)		
原文作者	Sean Barnum	原文发布日期	2014 年 2 月 20 日
作者简介			
原文发布单位	MITRE		
原文出处	https://stixproject.github.io/		
译者	小蜜蜂公益翻译组	校对者	小蜜蜂公益翻译组

“安全加”社区

小蜜蜂公益翻译组

目录

摘要

对组织来说，获得网络威胁情报能力越来越必要，而成功获取该等能力的关键要素是与合作伙伴、友商及所信任的其他人进行信息共享。网络威胁情报和信息共享可帮助组织聚焦庞杂的网络安全信息，并对数据的使用进行优先级排序，组织要处理此类信息，就必然需要标准化的、结构化的信息表达。STIX 指“结构化威胁信息表达”，是由多人群策群力共同定义、开发的描述结构化威胁信息的标准化语言，目前处于快速演进中。STIX 语言用以描述各种网络威胁信息，表达准确、灵活，具有可扩展性，可自动化，并易于理解。虽然是个较新的标准，且处于发展阶段，全球许多网络威胁相关组织及群体正积极采用或考虑采用 STIX。欢迎各方人士通过 STIX 网站、Email 讨论清单及其他合作论坛踊跃加入这个开放、合作的群体，一起推动 STIX 的发展。

反馈

STIX 的成功离不了各群体的输入。如对本文件或其他 STIX 文档有任何意见、问题、建议，可通过邮件发送至 stix@mitre.org。

1 引言

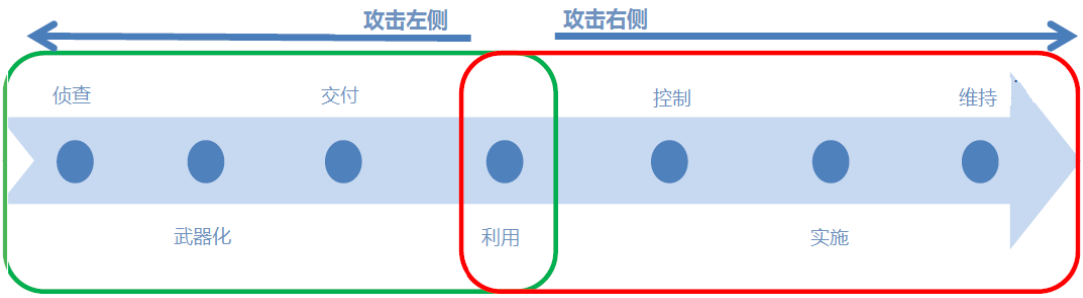
网络威胁信息共享与梳理需要基于多人协作开发的标准，该标准应不断完善与细化。本文即为这一过程中产生的文档。STIX 的形成得益于来自各行业、学术界与政府的组织与专家的反馈和积极参与，包括安全运营中心、CERT、网络威胁情报单位网络威胁信息的消费者与生产者、安全主管人员与决策人员以及大量活跃的信息共享群体，共享模型多种多样。HS-SEDI 代表美国国土安全部，协调 STIX 工作，欢迎各方踊跃加入 STIX 社区。

2 背景

网络安全是一个复杂的领域，涉及各方面问题，今后只会越来越复杂。人们对于复杂的技术越来越依赖，与此同时，威胁环境不断恶化，速度之快令人心惊。传统的网络安全方法关注的是内部对于漏洞、缺陷与配置的理解与处理，这很有必要，但还不够。对于当今与未来威胁的有效防护还需要对外部因素给以同样的关注，了解攻击者的行为、能力与意图。内外协调，知己知彼，才能直击威胁本质，作出明智决策。

现下不断演变的威胁环境使攻击场景愈加复杂。除了商业化威胁，一些过去罕见的高级能力现在也很普遍了。攻击者并不仅仅发动大规模的破坏行动（如几年前的 Storm 蠕虫爆发），反而常会低调行事，分阶段发动一些定向攻击，以实现特定战术目标，在企业网络中长期潜伏。

要有效理解这种较新的攻击场景及其防护措施，可从“攻击链[1]”着手，因为攻击链反应了攻击的各个步骤。如下所示，攻击分成几个步骤进行，最终攻击者在被害者网络中建立了据点。这是现在复杂的高级持续威胁（APT）的惯用伎俩。APT 源起方一般为国家，但是 APT 攻击也会被用以网络犯罪、金融威胁、工业间谍、黑客行动与恐怖活动。



网络攻击链示例

APT 的目的是长期潜伏，造成持续伤害，显然也有这个能力。这就促使网络安全防护由传统的被动回应转变为主动出击。漏洞被利用后再进行响应，代价高昂，因为效果有限，根除攻击据点也要花费很大力气。要实现主动防御，网络防护者需要提前（最好在上图所示攻击链的利用阶段之前，也就是攻击左侧）阻止攻击者，从根本上改变游戏性质。移到攻击左侧要求防护方的防护策略由事后调查与响应转变为受网络威胁情报驱动。

传统的情报有助于了解敌方能力、行动以及意图，网络领域的情报也具有同样功能。网络情报用于了解信息，归纳信息的特征，比如：已发生和可能发生哪些攻击行动、如何检测、识别和缓解这些攻击、相关威胁源起方是谁，试图达到什么目的、从其已利用和将来可能利用的策略、技术与过程（TTP）来看，他们具备哪些能力、他们可能要利用哪些漏洞、错误配置或缺陷、他们曾经采取了哪些行动等等。

全面了解攻击者所造成的威胁可进行更有效的决策支撑，确定行动优先级，更可能彻底打破攻防双方之间的平衡。根据 Hutchins、Cloppert 及 Amin[9]：

> “情报驱动的计算机网络防护（CND）使网络安全更具韧性。APT 源起方从本质上说是不停地进行入侵，根据每次入侵的结果（成功或失败）调整行动。在攻击链模型中，只要有一项缓解措施击破了链条，阻止了攻击者，后续任何相同动作都会被防护方识别及利用。”
>
> “通过这个模型，防护方可制定弹性的缓解措施，并对新技术或流程的投资作出明智决策。”
>
> “若防护方的防护快于攻击方的演进，攻击方则需要提高成本以达到自己的目标。这个模型表明，与传统认识相反的是，攻击方与防护方相比并不具有内在优势。”

网络威胁情报本身就是一个挑战，因为组织单凭一己之力无法从内部获取到足够的相关信息，准确感知威胁情况。要克服这种局限性，需与可信合作伙伴与团体进行相关的网络威胁信息共享。通过信息共享，每个合作伙伴都可能会从理论和实践上更彻底地理解威胁情况，知晓识别攻击者所要获取的具体信息。A 组织

1 http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

今天面临的威胁可能就是 B 组织明天所要面临的威胁，尤其是当 A 和 B 同为某个攻击者的攻击目标时。若 A 组织基于自己对某个威胁的了解与观察总结出网络威胁指标[2]，并将其作为个人实战经验进行分享，B 组织则可以利用这个信息在攻击发动前（攻击链上的攻击左侧）解决这个威胁。

鉴于威胁情况变得日益复杂、事件发生的速度之快以及网络威胁情报与威胁信息共享中所涉及的海量数据，采用自动化处理以辅助人类分析或以机器速度实施防护措施是有效对抗攻击的前提。自动化要求输入高质量信息。高防护能力大多无法基于同类架构形成，而是从各种迥异的产品及系统中获得。将所有这些因素结合起来要求标准化、结构化的威胁信息表达方式，以尽可能使更多的信息源群体贡献、利用信息，而无需事先知道谁会提供什么信息。

威胁共享组织面临的一个挑战是要具有构筑网络威胁信息的能力，同时又不失人类在共享中的判断与控制力。许多情况下，组织交换信息时希望信息既是人类可读，又是机器可解析的。多数信息共享项目都可以满足这个要求，使组织不仅可以使用数据而且在情报收集流程中可以访问数据。情报流程主要由人类情报分析师驱动，这类分析师关注的是不适于自动化的分析类型或要求人类进行的决策，第二种情况要求有人类互动，以便分析师可通过读取威胁信息而直接感知威胁态势并了解威胁情境。此外，因为共享威胁信息的质量参差不齐，情报分析师常要基于信息来源及信息产生方法评估信息的准确性。

由于上述因素，需要对威胁信息进行结构化的表达，这种表达方式应该清晰、灵活、可读，并且可以自动化，具有可扩展性。本文简要介绍了由多人群策群力共同开发的针对这个问题的解决方案，即结构化威胁信息表达（STIX）。

2 网络威胁指标：与情境信息结合的一组网络可察物，用以表示一个具体的网络安全环境下的重要工件及 / 或行为。

3 现用方法

STIX 是较新的概念，但是网络威胁信息共享，尤其是指标，却早有实践。当前，管理、交换的信息一般极为微细、多变，不够成熟与准确。而标准化结构只关注整个问题的单一方面，彼此独立或缺乏始终如一的灵活性。许多现有的指标共享活动是人与人之间通过 Web 门户或加密电子邮件对于潜在指标非结构化或半结构化描述的交流。较新的趋势是机器之间对于适用已知攻击模型的相对简单的指标数据集的传递，例如，研究与教育网络信息共享与分析中心（REN-ISAC）的安全事件体系及其集体情报框架部件、华盛顿州的公共区域信息安全事件管理（PRISEM）、能源部的网络联合模型（CFM）以及 CERT.FI 与 CERT.EE 的 AbuseHelper。

比较而言，STIX 旨在扩展指标共享，对表达更为准确的各类指标和其他各种网络威胁信息进行管理和广泛交流。

现今，网络威胁信息的自动管理和交换常与特定的安全产品线、服务产品或特定人群解决方案相关。STIX 可跨组织、人群、产品 / 服务共享全面、丰富和可靠的网络威胁信息。

4 发展历史

STIX 最初源于针对开发网络威胁指标表达标准的讨论，参与讨论者为 IDXWG 邮件名单上的安全运营及网络威胁情报专家，这份名单由美国计算机应急响应小组（US-CERT）与 CERT.org 在 2010 年拟定，以讨论网络安全事件的自动化数据交换问题。经过讨论，产生了粗略的结构化威胁信息架构图。该架构图的初始用途是厘清结构化网络威胁指标应包含的信息类型以及其他相关架构中应定义的信息类型，它划定了大致范围，这样便可以对其进行初步裁剪，形成结构化网络威胁指标表达。随着网络威胁指标概念及初始架构的成熟，会有越来越多的人去充实结构化威胁信息架构的其他部分。完整 STIX 架构的 XML Schema 实现结合了网络威胁指标表达等元素，是上述讨论的成果，反映了动态发展、不断壮大的群体对开发 STIX 语言所做的持续努力。

5 何为 STIX？

STIX 是所有相关各方共同开发的语言，用以规范、获取、表征、交流标准化的网络威胁信息。STIX 采用结构化的方式，为更有效的网络威胁管理流程和应用自动化提供支撑。

各种概要网络安全用例多依赖下述信息活动：

- 分析网络威胁；
- 明确网络威胁的指标特征；
- 管理网络威胁响应活动；
- 共享网络威胁信息。

STIX 为各种用例之间传递结构化的网络威胁信息提供了一个通用机制，增强了一致性和互通性，提升了效率和总体态势感知能力。

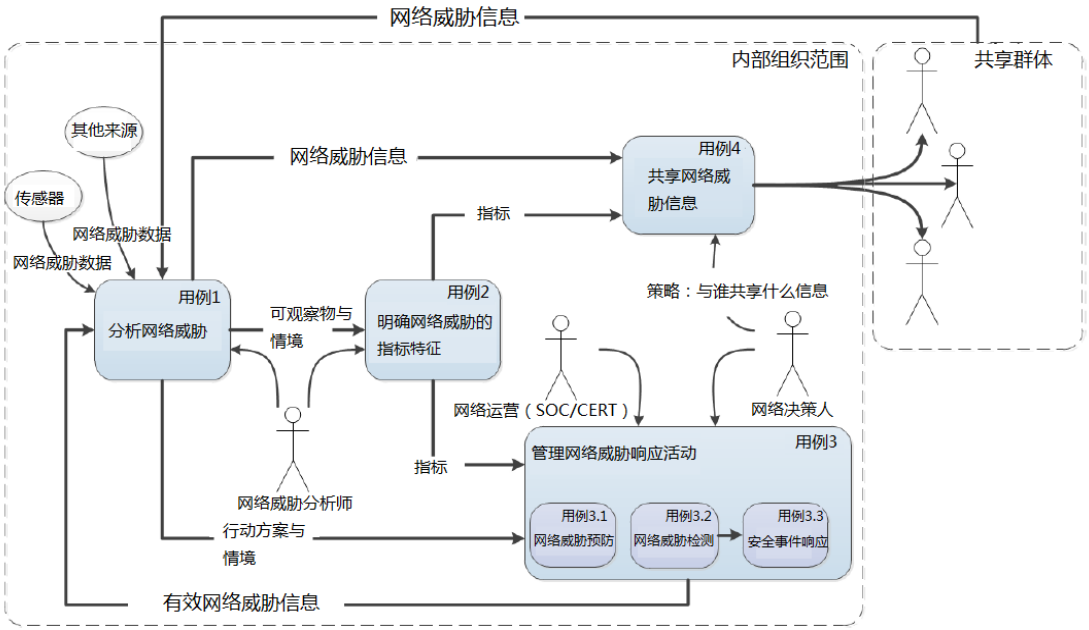
此外，STIX 作为统一架构，综合了各种不同的网络威胁信息，包括：

- 网络可察物；
- 指标；
- 安全事件；
- 攻击者的 TTP，包括攻击模式、恶意软件、利用程序、攻击链、工具、基础设施和锁定受害者等；
- 利用目标，例如，漏洞、缺陷或配置；
- 行动方案，例如，事件响应或漏洞 / 缺陷修复或缓解；
- 网络攻击活动；
- 网络威胁源起方。

STIX 作为一个综合方案既具有灵活性又具有可扩展性，可适用于任何单个用例。可酌情利用现有的标准化语言作为可选扩展，并在 STIX 语言中设计多个灵活机制。需特别指出的是，这一完全结构化的语言中，几乎任何一部分都是可选的。这样，单个用例仅需利用 STIX 语言中与其相关的部分（单个字段、整个语言或介于二者之间），而不受其他部分控制。STIX 能力的具体子集可以用 Profile 形式定义并约定，以便共享群体内部使用，或方便工具操作等等。

6 用例

STIX 用以支持网络威胁管理中涉及的各种核心用例，下图是这些用例的极简概要图。



STIX 针对的核心用例

6.1（用例 1）分析网络威胁

网络威胁分析师对各种手动、自动输入的网络威胁活动的结构化与非结构化信息进行评审，了解相关威胁的性质，对其进行识别和表征，这样，威胁的所有关联信息被充分描述并随时更新。这种关联信息包括威胁相关行动、行为、能力、意图、责任源起方等。基于对这些信息的理解与特征归纳，分析师接下来可明确关联威胁指标特征，建议威胁响应活动中应采取哪些措施，并 / 或与其他可信方共享此等信息。例如，对于潜在的钓鱼攻击，网络威胁分析师会分析、评估可疑的钓鱼邮件，分析所有的邮件附件与链接以确定其是否为恶意，评估钓鱼攻击目标与内容的普遍性，确定恶意附件是否打开过或包含链接，同时对所有的分析进行记录。

6.2（用例 2）明确网络威胁的指标特征

网络威胁分析师对于特定网络威胁及其情境与相关元数据的可观察特征明确规定其表达方式，并对特征及其匹配结果进行解释、处理与应用。这可以手动完成，也可以借助于自动化工具和结构化实例威胁信息完成。例如，在确定钓鱼攻击发生后，网络威胁分析师会通过分析钓鱼邮件获取相关可观察物信息（如源 / 目的地址、真实源、主题、嵌入 URL、附件类型、特定附件等），识别钓鱼攻击中发现的相关 TTP，对攻击进行攻击链关联，合理分配指标的置信度，确定合适的处理建议，生成指标相关的自动化规则（如 Snort、YARA、OVAL 等），确定使用哪种建议措施（若有），最后将所有这些信息整合，形成相关记录以用于共享（用例 4，见下文）及今后参考。

6.3（用例 3）管理网络威胁响应活动

网络决策者与网络运营人员共同防护、检测网络威胁活动，调查该活动的蛛丝马迹并作出响应。预防性行动方案可具有修复性，用以修复可能被利用的漏洞、缺陷或不当配置。在检测、调查了特定事件后，可以进行响应动作。例如，在确认钓鱼攻击发生并具有明确的指标后，网络决策者与网络运营人员进行合作，以充分理解环境中钓鱼攻击的影响（包括所安装或运行的恶意软件），对潜在行动方案进行成本与效用评估，实施恰当的预防或检测措施。

6.3.1（用例 3.1）网络威胁预防

针对已识别威胁，网络决策者评估潜在的行动方案，选择合适的实施措施。网络运营人员实施具体措施，以预防特定网络威胁，方法包括普遍应用缓解措施和基于对主要指标的预测性解释进行针对性缓解。例如，在确认钓鱼攻击发生并具有明确的指标后，网络决策者可评估针对此钓鱼攻击相关指标建议的预防性行动方案（如在邮件网关实施阻断规则），确定相关成本与风险，最后决定是否实施相关措施。若决定实施，具体的实施活动由网络运营人员承担。

6.3.2（用例 3.2）网络威胁检测

网络运营人员应用自动与人工机制来监控、评估网络运营，以检测特定网络威胁，无论威胁是通过取证确认已发生，还是通过动态态势感知发现正在进行中，还是通过对主要指标进行预测性解释预测将会发生。检测一般基于网络威胁指标特征。例如，在确认钓鱼攻击发生并具有明确的指标后，网络运营人员会根据确定的攻击指标收集特定可观察物特征，将其正确应用到运营环境中，以便钓鱼攻击发生时准确检测。

6.3.3（用例 3.3）安全事件响应

网路运营人员对检测到的潜在网络威胁进行响应，调查已发生或正在发生的事件，尝试识别并归纳实际威胁的特征，并在可能情况下实施特定的缓解或纠正措施。例如，在确认发生钓鱼攻击后，网络运营人员可进行调查活动以确定钓鱼攻击是否在目标环境成功造成负面影响（如，恶意软件是否已安装或运行），若答案肯定，则尽量详细描述这些影响（如，哪些系统受到恶意软件影响、泄露了哪些数据等等）。在了解了影响之后，网络运营人员会采取合理的缓解或纠正措施（如，清理及恢复系统、封堵外泄渠道等等）。

6.4（用例 4）共享网络威胁信息

网络决策者制定策略，确定与哪些人共享何种类型的网络威胁信息，如何基于商定的信任框架处理这些信息，以维持合理水平的一致性、情境描述及控制。接下来是实施策略，共享恰当的威胁信息指标以及其他的网络威胁信息。例如，在确认钓鱼攻击发生并具有明确的指标后，可基于网络决策者事先确定的策略同可信方或群体自动或手动共享相关指标，这样共享方所获取的知识亦可惠及他人。

7 指导原则

定义网络威胁信息的结构化表达时，STIX 团队力求坚持和落实社区一致认为必要的核心指导原则这些指导原则如下：

7.1 清晰表达

为全面支持网络安全领域中各种威胁相关用例，STIX 针对所有目标用例（而非特定的一、两个用例），提供一体化的清晰表达 STIX 旨在为网络安全领域的相关信息提供全面清晰表达。

7.2 集成，而非复制

对于 STIX 范围中涉及的已有充分标准化表达的结构化信息概念，默认提供合理机制将这些表达集成至 STIX 整体架构中，而不是多余的复制。

STIX 直接采用以下规范：

- 网络可观察表达规范（CybOX™）

http://cybox.mitre.org/

STIX 1.1 版本提供了适当的松耦合机制及默认实现，以利用以下规范：

- 通用攻击模式枚举和分类（CAPEC™）

http://capec.mitre.org/

- 恶意软件属性枚举和特征描述（MAEC™）

https://maec.mitre.org/

- 通用漏洞报告框架（CVRF）

http://www.icasi.org/cvrf

- OASIS 客户信息质量（CIQ）xPRL

https://www.oasis-open.org/committees/ciq/

7.3 灵活性

各种用例不一而足，各种信息良莠不齐，因此，STIX 特意设计为尽可能地具备较大灵活性 STIX 允许用户只利用特定情境相关的那部分标准表达，而非全部表达，尽量避免必选特性。

7.4 扩展性

为支持具备各种潜在表达细节的一系列用例，并方便通过群策群力实现语言改进和演进，STIX 在设计时特意嵌入了扩展机制，从而实现在特定领域的应用、本地使用、用户驱动的改进和演进，并方便集中改进和演进。

7.5 自动化

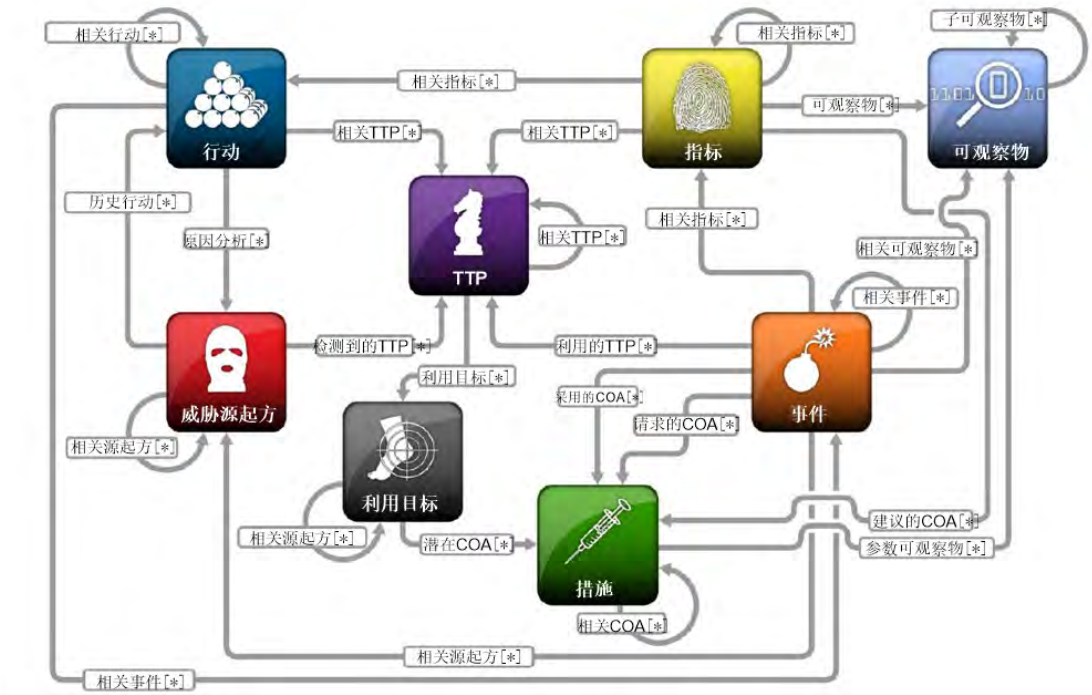
STIX 在设计时力求优化结构，保持一致，以支持机器自动化。

7.6 可读性

STIX 在设计时有意使其内容结构既可由机器利用和处理，还尽可能地实现人类可读人类可读性非常必要，因为这使 STIX 在开发和应用早期更加清晰且易于理解，而且未来可在各种环境中持续使用。

8 架构

下面的 STIX 架构图展示了网络威胁的核心概念（作为可复用的独立构造），并基于构造的内在含义和内容描绘了他们之间的关系构造图标之间的连接箭头表示的是构造之间的关系，具体表现形式为箭头尾部构造的内容元素。箭头尾部的构造为箭头头部构造的概念性类型，箭头头部构造的 STIX 实现仅为建议，而非强制要求每个箭头上方括号中的星号表示每个关系可存在 0 至多次每个构造的结构化内容在语言实现（目前为 XML Schema）中进行详细描述下面简要介绍八个核心构造，包括可观察物、指标、事件、TTP、利用目标、措施、行动、威胁源起方，以及交叉的数据标示构造。



STIX V1.1 架构

9 STIX 结构

9.1 可观察物

可观察物是 STIX 架构中的基础构造可观察物是计算机和网络的相关操作的状态属性或可衡量的事件文件（名称、哈希和大小等）、注册表项值、启动的服务或发送的 HTTP 请求均为可观察物的简单实例。

STIX 利用 CybOX 表达可观察物。

CybOX 是用于编码和传达网络可观察物相关的标准化可靠信息，包括可操作的网络领域中观察到的动态事件及状态措施属性 CybOX 跟 STIX 类似，不针对单个网络安全用例，而是具备足够的灵活性，对需具备网络可观察物处理能力的所有网络安全用例提供通用方案此外，CybOX 的灵活性还体现在以下两方面:在可操作情境中对可衡量网络可观察物实例进行准确描述，还可能被观察和分析的潜在可观察物进行抽象描述。

9.2 指标

指标描述了特定可观察物模式以及用于表示网络安全情境中工件和 / 或需关注的行为的情境信息这些信息包括一个或多个可观察物的模式。这些模式可能映射到相关的 TTP 情境，并提供以下项目的其他相关元数据，如指标断言的置信度、处理限制、有效时间窗口，潜在影响、指标出现次数、用于检测的结构化测试机制、相关行动、建议的方案、相关指标以及指标来源等。

鉴于当前标准表达方法存在限制，STIX 基于集体智慧构建，采用最佳实践定义新的指标结构表示指标信息。

9.3 安全事件

安全事件是影响组织的指标的独立实例，并包含事件响应调查中发现或确定的信息。

安全事件数据包含时间相关信息、相关方、受影响的资产、影响评估、相关指标、相关可观察物、利用的 TTP、涉及的威胁源起方、预期影响、入侵性质、所需的响应行动、采取的响应行动、描述的置信度、处理建议、事件信息来源、采取行动的日志等。

鉴于当前标准表达方法存在限制，STIX 基于集体智慧构建，采用最佳实践定义新的事件结构表示事件信息。

9.4 策略、技术与过程（TTP）

TTP 描述了网络攻击者的行为或攻击方法 TTP 是传统军事的一个术语，用于描述敌人发动了哪些攻击行动以及更详细地阐述敌人如何实现这些行动例如，利用恶意软件窃取信用卡凭证就是一个有关策略的简单例子此例中的相关技术（更详细的描述）可能为向潜在受害人发送特定邮件。邮件附件包含恶意代码，一旦受害人打开附件，这些代码就会执行，在受害人进行键盘操作时获取银行卡信息，通过 HTTP 和命令与控制服务器通信，传送信息相关过程（更为详细的描述）可能为进行开源研究，识别容易上当受骗的个人，编写有

说服力的社会工程邮件和文档，构建恶意软件 / 漏洞利用程序绕过当前防病毒检测，注册 mychasebank.org 域名构建命令与控制服务器，利用 Gmail 邮箱 accounts-mychasebank@gmail.com 向受害人发送邮件。

TTP 包括攻击者采用的具体攻击行为（攻击模式、恶意软件、漏洞利用程序）、利用的资源（工具、基础设施、受害人）、受害人相关信息（在何地利用了哪些受害人以及如何利用受害人）、相关利用目标、预期影响、相关攻击链阶段、处理建议、TTP 信息来源等。

TTP 在网络威胁信息和情报方面发挥核心作用 TTP 与指标、事件、行动和威胁源起方存在关联此外，TTP 还与利用目标存在密切联系，这些利用目标为 TTP 试图利用的特定目标。

鉴于当前缺乏标准方法，STIX 基于集体智慧构建，采用最佳实践定义新的 TTP 结构表示 TTP 信息而部分 TTP 构造基于所定义的扩展点利用其它现有标准方法，对攻击行为等进行详细描述，介绍攻击模式、恶意软件和资源（包括工具和基础设施）此外，可利用 CAPEC 对 TTP 攻击模式、MAEC 对 TTP 恶意软件进行结构化描述，并利用 CybOX 对工具和基础设施进行描述。

9.5 行动

行动是威胁源起方实施其意图的实例，其意图可通过一系列事件和 / 或 TTP（可能是跨组织的）观察到从结构上看，行动可包括据推测攻击者可能想要达到的影响、行动利用的相关 TTP、被视为行动的一部分的相关事件、对发动行动的威胁源起方进行分析、行动相关的其他行动、总体意图描述及行动描述的置信度、采取的响应活动、行动信息的来源和处理建议等。

鉴于当前缺乏标准方法，STIX 基于集体智慧构建，采用最佳实践定义新的行动结构表示行动信息。

9.6 威胁源起方

威胁源起方指发动网络攻击威胁的恶意行动者（或攻击者）。网络攻击威胁包括推测的意图和所观察到的历史行为从结构上看，威胁源起方描述包括身份、推测的动机和预期影响、之前观察到的威胁源起方采用的 TTP、被视为与威胁源起方有关联的历史行动、其他相关威胁源起方、处理建议、威胁源起方描述的置信度以及威胁源起方信息的来源等。

鉴于当前缺乏标准方法，STIX 基于集体智慧构建，采用最佳实践定义新的威胁源起方结构表示威胁源起方信息。

9.7 利用目标

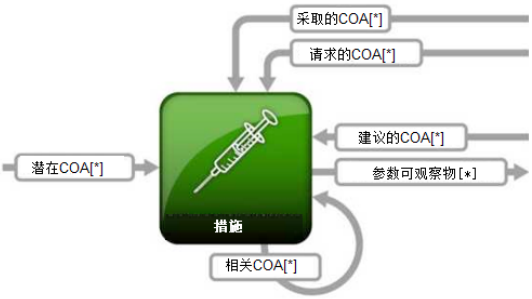
“利用目标”指被威胁源起方 TTP 利用的软件、系统、网络或配置中的漏洞或缺陷。结构上，利用目标包括漏洞标识或描述、缺陷标识或描述、配置标识或描述，潜在行动方案、利用目标信息来源、处理建议等。

鉴于当前的标准方法缺乏普遍适用的描述，STIX 基于集体智

慧构建，采用最佳实践定义新的利用目标结构表达利用目标信息。然而，部分利用目标结构基于所定义的扩展点利用其他现有的标准方法，来描述漏洞、缺陷和配置。通用漏洞披露（CVE®）和开源漏洞数据库（OSVDB）中的标识符用于识别公开披露的漏洞。通用漏洞报告模板（CVRF）格式可详细描述 CVE 或 OSVDB 之外的漏洞，甚至可能用于描述零日漏洞。通用缺陷枚举（CWE™）中的标识符可用于识别缺陷。通用配置枚举（CCE™）中的标识符可用于识别配置问题。

9.8 行动方案（COA）

COA 是解决威胁的具体措施，可纠正或预防利用目标，以应对或缓解安全事件的潜在影响。在结构上，COA 包括网络威胁管理中的相关阶段（例如，修复利用目标或响应安全事件）、COA 类型、描述、目的、结构化表达（如入侵防护规则或自动修补 / 修复）、可能的影响、可能的成本、预估功效、可观察物参数及处理建议。



鉴于当前的标准方法缺乏普遍适用的描述，STIX 基于集体智慧构建，采用最佳实践定义新的 COA 结构表达行动方案信息。

9.9 数据标记

不同的核心 STIX 构造有一个相同的要求，即可以用数据标记表示特定要求，比如，虑及网络威胁信息的潜在敏感性所做的处理限制。该构造不是 STIX 架构图中的独立实体，而是上述所有顶级结构中的一个交叉结构。目前，对数据标记的标准化方法还未达成广泛共识。不同群体有不同的方法，动机和使用场景也不同。STIX 并没有采用单一的标记方法（如交通灯协议（TLP）[3]）并试图强迫大家接受它，而是采取灵活通用的方法。

STIX 中定义的数据标记结构很灵活，原因如下：其一，实例独立于被标记的结构（指向其位置），而不是随处嵌入，这样通常低效且难以更新和完善。其二，在定义和使用数据标记结构时，均以基础类型结构为母体。这样，就可以使用不同的标记方案，并且当与上述独立规范结合时，方便地使用不同用例或不同群体的多种标记方案来标记任何数据结构。这一数据标记结构已初步利用 XML 结构（XSD）实现，并可能被用于 STIX 的整个 XML 实现过程中，以及任何其他基于 XML 的结构化表达。

3 http://www.us-cert.gov/tlp/

10 实现

STIX 的初步实现将 XML Schema 作为一个无处不在的、便携式的和结构化的机制，相关群体可就其进行详细讨论、协作和细化。它还提供一个实用结构，在结构化威胁信息管理和共享方面提供真实原型和概念验证（PoC）实现。各种支持工具的开发将会鼓励和支持促进这种语言的实际使用，如编程语言绑定、表达转换平台、API 等。只有通过相关群体专家的适当协作迭代并使用真实数据和用例审查，实用有效的解决方案才能得以发展。

语言结构也有所规划，用于实现独立规范。这能够促使其他潜在的实现，包括语义网络（RDF/OWL）、JSON-centric 和 ProtocolBuffers 等。

11 用法

STIX 已引起各组织和群体的极大兴趣，这些组织和群体正面临承担或支持网络威胁情报和信息共享的挑战。已选择开始使用 STIX（或其组件）来传递网络威胁信息的组织包括：

- 美国国土安全部（DHS）在一些关键领域（包括指标信息的可信自动化交换（TAXII）[4]）使用 STIX，允许网络安全和通信办公室（CS&C）及其政府和私营部门的合作伙伴使用安全的自动化机制来交换 STIX 定义的数据元素和关系。通过使用 STIX 可实现快速检测、防护和减轻网络威胁，并在可能的情况下，将此过程中的关键要素实现自动化。目前，TAXII 的初步概念验证正在进行中。
- 目前，美国国土安全部网络信息共享与合作项目（CISCP）正在利用 STIX 将所有有效的威胁信息向项目合作伙伴发布。
- 美国国土安全部国家网络安全和通信集成中心（NCCIC）正在分阶段开发与网络威胁相关的可操作 STIX 产品。
- 在 2012 年第二季度，金融服务信息共享和分析中心（FS-ISAC）同意其成员在在金融服务领域使用 STIX 架构（包括 CybOX）来实现网络威胁信息共享。截至 2013 年 5 月，FS-ISAC 使用 STIX 维护业务威胁信息库，并提供给其所有的 4200 个成员组织使用。
- 2013 年 7 月，微软宣布将通过其新的 MAPP for Responders 计划把 STIX 用于威胁信息共享。
- 2013 年 9 月，惠普发布了一款新产品 Threat Central，即基于 STIX 的威胁情报共享环境。
- 日本情报处理推进机构（IPA）目前正积极开展将 STIX 架构（CybOX 和 MAEC 等）元素用作网络可察物和威胁信息的国际交换格式的可行性研究。

此外，大量的美国和国际公对公、公对私和私对私的网络威胁信息共享群体以及支持该领域的一些厂商正积极研究运用并原型化 STIX 及其组件。

4 http://taxii.mitre.org

12 结论及未来工作

目前，迫切需要有新的和更多的外向合作方式，用于网络安全防御。网络威胁情报和网络威胁信息共享作为前沿性的创新方法，在打破攻击者和防护者之间的平衡方面有很大的潜能。成熟有效的网络威胁情报和网络威胁信息共享的核心要求是开放标准化、结构化的网络威胁信息平台的可用性。STIX 是集体合作的结果，它依据指导原则提供的表达方式可最大程度地优化表现性、灵活性、可扩展性、自动化和可读性。STIX 提供全面的网络威胁信息（包括可观察物、指标、安全事件、TTP、利用目标、行动方案、威胁源起方和活动），从而为广泛的网络安全防护用例提供支持。虽然相对较新且处于发展阶段，STIX 已引起广大利益相关者和社区（包括公共和私营的）的极大兴趣。截止目前，有证据表明，STIX 很可能在解决网络威胁信息问题是有效实用的，并可以为从业者群体和支持实体所接受。

随着关注度的提升和初步实际应用，可以预见的是，集体对 STIX 工作的参与程度将不断提高。集体工作将集中于评估和完善语言的原理实现（最终形成独立于实现的语言规范）、持续原型化和使用，以及支持工具的开发。此外，还将建品牌推广和应用计划，以推动和支持新兴的产品、服务和信息源的生态系统。这些产品、服务和信息源可被用于解决网络威胁信息共享问题。

欢迎和诚邀有意者参与此项工作，加入协作社区，共同讨论、开发、改善、使用和支持 STIX。欲了解更多信息，请登录 STIX 网站（http://stix.mitre.org/）。问题或建议可发送至 STIX 团队（stix@mitre.org）或 STIX 讨论清单上的 STIX 社区（http://stix.mitre.org/community/registration.html）。您可登陆 STIX Project GitHub 网站（https://github.com/STIXProject）了解完整的模式实现、工具和问题跟踪。

13 致谢

HS SEDI 作为 STIX 工作的社区协调者及本文编辑人员，其工作得到了了美国国土安全部的支持。虽然本文所述工作是基于很多来自不同组织的个人对这些主题做出的努力、建议和沟通，但这里要特别感谢那些费时对本文做出评审和评论的人员。

对 STIX 讨论做出贡献的组织包括（以下仅为部分示例）：

- MITRE 公司
- 美国计算机紧急响应小组（US-CERT）
- 美国国土安全部网络信息共享与合作项目（CISCP）
- 美国国土安全部国家网络安全和通信集成中心（NCCIC）
- 增强共享态势感知（ESSA）
- 国家标准与技术研究院（NIST）
- 金融服务信息共享与分析中心（FS-ISAC）
- 国家计算机网络应急技术处理协调中心（CERT/CC）
- 研究与教育网络信息共享和分析中心（REN-ISAC）
- 工控系统信息共享和分析中心（ICS-ISAC）
- 电力部门信息共享与分析中心（ES-ISAC）
- 国家卫生信息共享与分析中心（NH-ISAC）
- 国防部网络犯罪中心（DC3）
- 国家网络调查联合特遣队（NCIJTF-AG）
- 美国存管信托和结算公司（DTCC）
- 高盛
- 美国运通
- USAA
- 通用电气
- 西门子
- Visa
- 微软
- 惠普
- Check Point
- CrowdStrike 公司
- FireEye/Mandiant
- CyberIQ
- LookingGlass
- iSIGHT Partners
- Red Sky Alliance
- Damballa
- Esentire
- Tripwire
- 威瑞信
- Verizon
- 洛克希德·马丁
- 美国通用动力公司
- Northrop Grumman

参考

1. Cyber Observable expression (CybOX). URL https://cybox.mitre.org
2. Common Attack Pattern Enumeration and Classification (CAPEC). URL https://capec.mitre.org
3. Malware Attribute Enumeration and Characterization (MAEC). URL https://maec.mitre.org
4. Common Vulnerabilities and Exposures (CVE). URL https://cve.mitre.org
5. Common Weakness Enumeration (CWE). URL https://cwe.mitre.org
6. Common Configuration Enumeration (CCE). URL https://cce.mitre.org
7. Open Source Vulnerability Database (OSVDB). URL http://www.osvdb.org
8. Common Vulnerability Reporting Framework (CVRF). http://www.icasi.org/cvrf/
9. E.M. Hutchins, M.J. Cloppert and R.M Amin PH.D., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Intfl Conf. Information Warfare Sec^rit;y (ICIW 11), Academic Conferences Ltd., 2010, pp. 113-125; URL: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
10. Luc Dandurand，Emmanuel Bouillon and Philippe Lagadec, “High-level Requirements for a Cyber Defence Data Collaboration and Exchange Infrastructure，’’ Reference Document 3175, NATO Consultation, Command and Control Agency, April 2011.
11. “TAXII: The Trusted Automated eXchange of Indicator Information，” U.S. Department of Homeland Security
12. “Cyber Information-Sharing Models : An Overview，” MITRE Corporation，May 2012.
13. “Active Defense Strategy for Cyber，” MITRE Corporation，July 2012.
14. “A New Cyber Defense Playbook，” MITRE Corporation，July 2012.
15. IDXWG@NICWG.ORG, Oct 2011 - May 2013
16. Traffic Light Protocol (TLP). URL http://www.us-cert.gov/tlp/
17. Julie Connolly，Mark Davidson，Matt Richard，Clem Skorupka， “The Trusted Automated eXchange of Indicator Information (TAXII™)，” November 2012. http://taxii.mitre.org/about/documents/Introduction_to_TAXII_White_Paper_November_2012.pdf

使用 STIX™ 规范
网络威胁情报信息

安全加社区

公益译文项目 2017

网络安全公益译文项目旨在分享国外先进网络安全理念，将网络安全战略性文档翻译为中文，促进国内安全组织在相关方面的思考和交流。该项目由安全加社区发起，安全加社区是国内的网络安全社区，社区欢迎网络安全人士的加入，并致力于交付网络安全问题的解决能力。